



2nd Annual
MidPoint Community Meetup

Governance of Non-Human Identities

Agenda

- Introduction to Non-Human Identities (NHI)
- Governance of NHI
- NHI in midPoint
- Conclusion and recommendation



From Human to Non-Human Identities (NHI)?

- Human identities are prime
- NHI are naturally occurring
- Modern IT is mostly automatized
- Blurring the differences
 - Devices, services, agents acting as a user
- Zero trust principles
- Embrace non-human identities



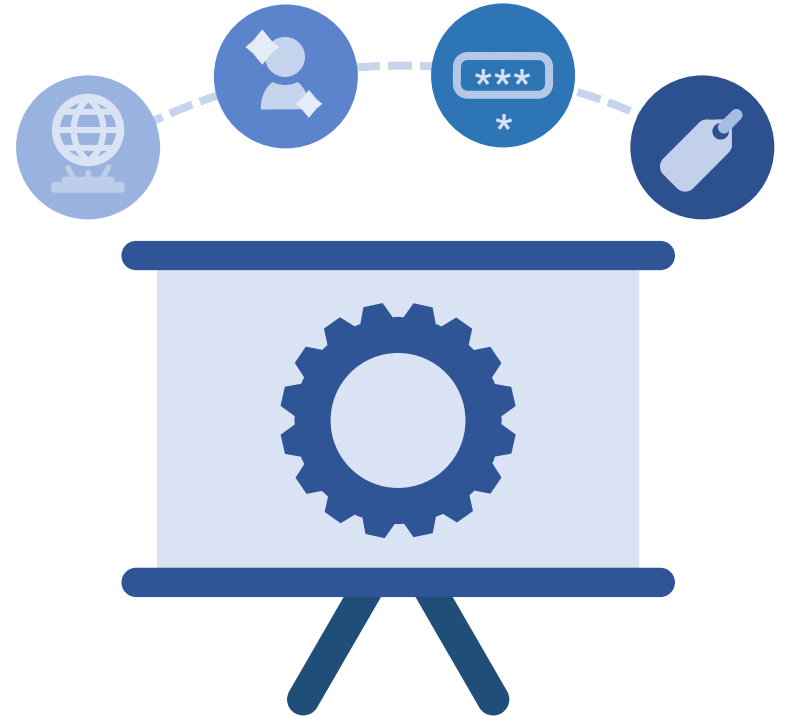
Why Non-Human Identities?

- The number is rising
 - Estimates are 20-50x more than human identities
- Often overlooked
 - Both life-cycle and usage
- Huge potential attack surface
 - Privileged by design
- Harder to manage
 - Scale
 - Shared ownership



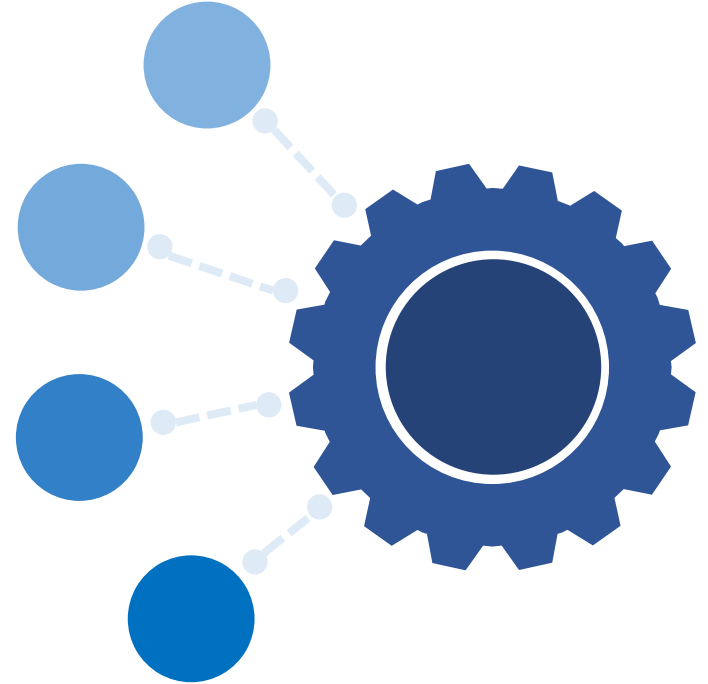
Types of Non-Human Identities

- Service accounts, system accounts
- Devices
- Internet of things
- Applications, micro-services
- Agents, bots
- Integration code, CI/CD
- Workload
- ...



Typical Approach to Non-Human Identities

- Low-level approach to NHI management
- Security
- Credential management
- API protection
- Monitoring, risk assessment
- There are many specialized solutions for it



What About Governance?

- Governance as an essence of managing NHI
- A high-level approach to NHI governance
- Why does NHI exist? (purpose)
- Who is responsible? (ownership)
- What can NHI do? (authorization)



Modeling NHI in midPoint

- Service object
- Use archetypes
 - Different types of NHI
- Track ownership
 - Users, org. units
- Manage life cycle
- RBAC

The screenshot shows the midPoint user management interface. The top navigation bar includes the midPoint logo, a hamburger menu, and the text "All users". A sidebar on the left contains a navigation menu with options like "SELF SERVICE", "ADMINISTRATION", "Dashboards", "Users", "All users", "Persons", "Agents", "Devices", "Service acc.", "New user", "Org. structure", "Roles", "Services", "Policies", "Resources", "Cases", "Certification", and "Server tasks". The main content area displays a table of users with a search bar at the top. The table has columns for Name, Personal Number, Full name, Email, and Accounts. The data rows are as follows:

	Name	Personal Number	Full name	Email	Accounts
<input type="checkbox"/>	administrator		midPoint Administrator		
<input type="checkbox"/>	borgia		Cesare Borgia	cborgia@leonardo-workshop.org	
<input type="checkbox"/>	ci/cd-agent	NHI-4	CI/CD integration agent	it@leonardo-workshop.org	4
<input type="checkbox"/>	db-admin	NHI-6	SQL server administrator	it@leonardo-workshop.org	1
<input type="checkbox"/>	donatello	2	Donatello di Niccolo di Betto Bardi	donatello@leonardo-workshop.org	1
<input type="checkbox"/>	francis		King Francis I of France	king@kingdom.fr	1
<input type="checkbox"/>	hallway-scanner	NHI-5	Hallway scanner	scanner@leonardo-workshop.org	2
<input type="checkbox"/>	ldap-administrator	NHI-1	LDAP administrator	ldapadmin@leonardo-workshop.org	1

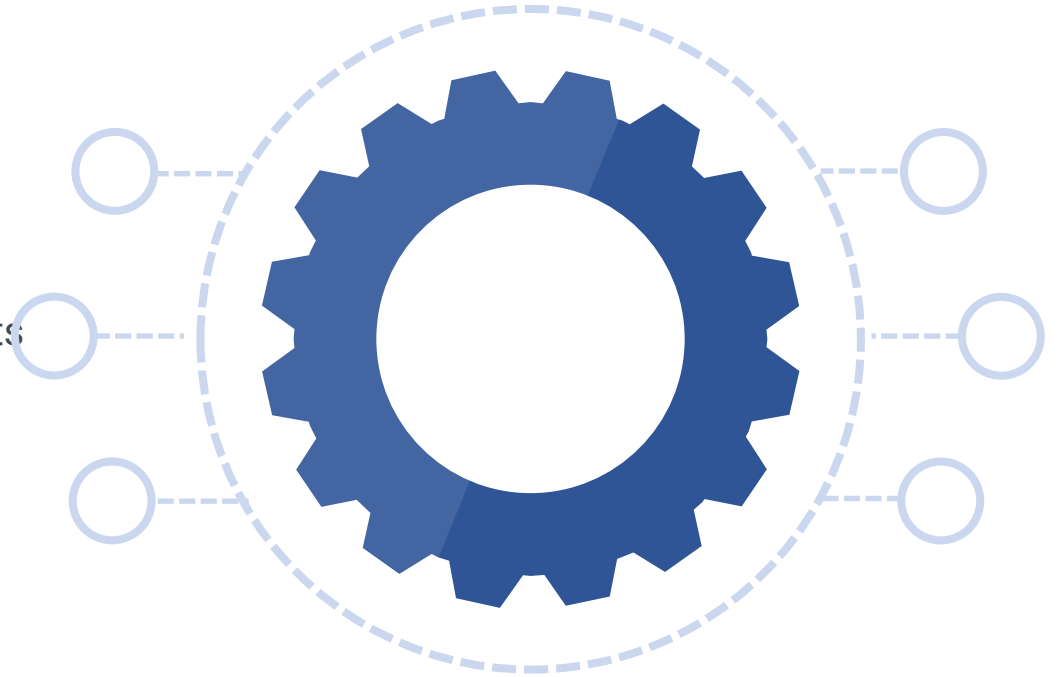
Lifecycle

- Standards lifecycle options
 - Manual management in midPoint
 - External source
- Approvals for creation and new accesses
- Lifecycle based on ownership
- Recertification of ownership



Discovery & Provisioning

- Using standard connectors
 - Use different kind / intent
- Manage accounts for access management
- Consider reaction on newly discovered accounts
 - Report
 - Disable
- Integrate with other NHI management tool
 - Make sure are accounts are managed



Conclusion

- Existing IGA principles are applicable to NHI
- You most likely have an IGA or IdM
- You can start by extending the existing IGA with NHI
 - Minimal initial investment
- Then you can continue with specialized tools or by extending NHI-related IGA processes
- **It is recommended to start with inventorization & ownership responsibility**



Evolveum

Thank you for your attention

Feel free to ask your questions now!



2nd Annual MidPoint Community Meetup